OPI DATE 07/08/98 APPLN. ID 79988/98
AOJP DATE 08/10/98 PCT NUMBER PCT/AU97/00888

AU9879988

INTI

(51) International Patent Classification 6 : H04L 9/14, 9/20, H04K 1/10 — A1

(11) International Publication Number: WO 98/32260

(43) International Publication Date: 23 July 1998 (23.07.98)

(21) International Application Number: PCT/AU97/00888

(22) International Filing Date: 30 December 1997 (30.12.97)

(30) Priority Data:
PO 4605 14 January 1997 (14.01.97) AU

(71) Applicant (*for all designated States except US*): COMMONWEALTH BANK OF AUSTRALIA [AU/AU]; 48 Martin Place, Sydney, NSW 1155 (AU).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): MAPSON, Michael, Joseph [AU/AU]; 69 Yalor Road, Bangor, NSW 2234 (AU).

(74) Agent: WATERMARK PATENT & TRADEMARK ATTORNEYS; Level 4, Amory Gardens, 2 Cavill Avenue, Ashfield, NSW 2131 (AU).

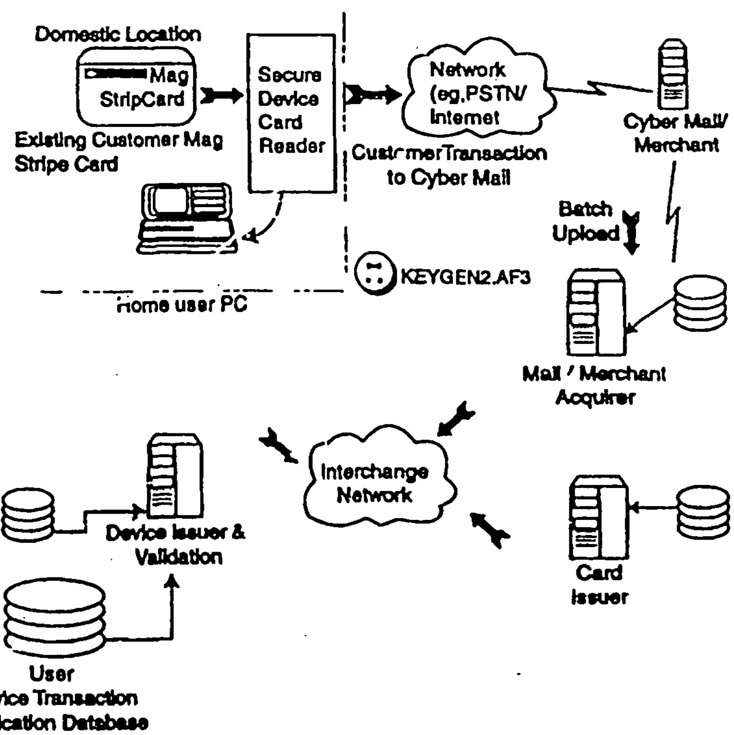
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: SECURE MESSAGING TABLE SYSTEM

(57) Abstract

The present invention relates to secure messaging using a telecommunications network or the like, particularly but not exclusively in environments where the message is intended to be carried over an unsecured telecommunications link. Without limitation, one application of the present invention is in financial transactions between a customer, vendor and financial institution. In essence, the present invention stems from the realisation that by providing second identifiers in association with the first identifiers, it is possible to determine whether transactions are valid or invalid.



SECURE MESSAGING TABLE SYSTEM

Technical Field

The present invention relates to secure messaging using a telecommunications network or the like, particularly but not exclusively in environments where the message is intended to be carried over an unsecured telecommunications link. Without limitation, one application of the present invention is in financial transactions between a customer, vendor and financial institution.

Background Art

Electronic messaging systems of various types have come into increasing use over the last decade. Such developments as widespread use of internal networks, and the increase of internet access and use, have contributed to this growth.

Secure messaging is traditionally carried out using one of several mechanisms. In one type of arrangement, exemplified by electronic funds transfer all terminals are uniquely identified, the lines are insecure, and session keys are generated for each transaction using real time on-line links between the terminal and the host. However, such a system is not suitable where messages may be received out of order, as in a packet based system, or where communications real-time links may be unreliable.

Another alternative is the use of asymmetric key encryption, such as RSA, in which a public key is disseminated, with the private key held only by the intended receiving party. A corresponding relationship needs to be established to allow for two-way communications. In such systems, the same key is used for numerous transactions, which creates a security risk over time - in other words, the key is not unique to any given communication.

It is an object of the present invention to provide a secure messaging system which allows for secure message transfer and verification, but where there is no real time link between the sender and the receiver, and messages or transaction data may be received out of order.

Summary of the Invention

According to a first aspect, the present invention comprises a system for securely communicating a message from a transmitting means to a receiving means, said transmitting means having a first unique identifier, said message including a second identifier generated by said transmitting means which is unique for each message, wherein said transmitting means encrypts said message, and generates a message block including said encrypted message and said first identifier in unencrypted form, said message block being transmitted, wherein said receiving means is enabled to decrypt the message using the first unique identifier, and includes a list of possible second identifiers for the transmitting means associated with the first identifier, and an indication of whether such second identifiers have been used, so that said message block is recognised as valid only if the second identifier associated with the message block has not previously been used.

In essence, the present invention stems from the realisation that by providing second identifiers in association with the first identifiers, it is possible to determine whether transactions are valid or invalid.

Preferably, the encryption is performed using an encryption engine contained within a secure hardware element of the transmitting means. For example, the transmitting means may comprise a secure smartcard reader in combination with the customer's smartcard, and a PC or similar device connected to a modem. Preferably, the encryption engine generates a unique key for each transaction, by operating a suitable function on one or more random or pseudo-random numbers generated by the transmitting means. This random number is in this case transmitted un-encrypted in the message block to the receiving means. The receiving means stores decryption information associated with the transmitting means, so that given the first unique identifier and the random number, the message can be decrypted. This provides a unique key for each message without the necessity for a real time link. However, the present invention may be implemented using an RSA or similar system, with the message identifier providing security to ensure that the message did originate from the transmitting means.

The present invention is particularly applicable to systems such as the internet, and more particularly to arrangements in which a secure transaction may pass through several parties before being presented to the intended recipient. An example of such an application is a payment instruction from a party to purchase goods via the internet. The fundamental relationship to effect the payment is between the customer and the financial institution which will pay the vendor. Hence, the customer may send a message block to the vendor, including unencrypted data such as the amount, the customer's financial institution, and the date, together with an encrypted confirmation of these details and confidential details such as a credit or debit card number, a PIN (personal identification number), transaction value and the customer's account details. The vendor may pass the message block to his bank, for later submission to the customer's bank. Alternatively, if the transaction has a small value, the vendor may store the message blocks and submit them as a batch to a bank or financial institution. In either case, the unique (second) identifier associated with each message allows the customer's bank to determine whether the transaction is legitimate or fraudulent. Certainly, any simple cloning of the message block will not succeed, as the clone will have the same message (second) identifier and hence be refused by the customer's bank.

Alternatively, the cloned message will be accepted by the customers financial institution in the event that it arrives at the financial institution before the genuine or delayed original message. The genuine delayed message may then be rejected on its arrival. However, the cloned message can only have achieved the same objective as the genuine message should have done, unless it was otherwise tampered. In the event it was tampered, the message decryption will fail and the allocated transaction number will not be recovered from the decryption. Thus if the clone message is tampered, it will fail. The genuine message will eventuate.

Other applications of the inventive system will be apparent to the reader.

Thus, the present invention provides a messaging system which allows for secure messages to be transmitted without any acknowledgment to the sender.

Brief Description of the Drawings

One illustrative embodiment of the present invention will now be described with reference to the accompanying figures, in which:

Figure 1 is a schematic overview of a general arrangement in which the present invention may be used;

Figure 2 is a block diagram illustrating one possible encryption process in the transmitting device;

Figure 3 is an example transaction certificate format;

Figure 4 is an example of a block message format; and

Figure 5 illustrates an exemplary algorithm for generating a transaction key.

Detailed Description

The present invention will be described with reference to a particular application, that of funds transfer over a communications network such as the internet. However, it will be understood that with suitable modifications the present invention is more broadly applicable. The design and details of the encryption system, and receiver and transmitter elements, are not essential in detail to the present invention - it is only their functionality which defines the present invention. Greater or lesser levels of encryption security may be used depending upon the wishes of the system implementer.

Referring to figure 1, the arrangement shown is one in which a domestic customer wishes to purchase goods or services from a cyber merchant - i.e. one accessible via the internet. The home user has a magnetic stripe or smartcard credit or debit card, a secure device card reader, and a PC and modem connected conventionally for internet access. Security functionality may be shared between a smart card and/or a card reader dependent on the capability of each item. The other parties shown are the merchant, which is the vendor; the acquirer, which is the financial institution with whom the merchant has a relationship; the card issuer, who has a relationship with the customer; and the device issuer, who supplied the secure device card reader. It will be appreciated that less complicated arrangements are possible where, for example, the device issuer is the card issuer, or the merchant and customer share the same financial institution.

A typical debit purchase transaction may operate as follows:

1. Customer selects item(s) for home purchase from the merchant's web site, and initiates purchase software between the merchant's site and the home PC. An applicable software "shopping" application exists, with hooks to import and export data to a Secure Device attached to, for example COM2. The import / export control between the application and the Secure Device will be a separate control protocol.

2. Customer has a mag stripe, linked or smartcard debit card.

3. Merchant provides purchase details - for example, merchant ID, value of transaction, and other relevant data. The merchant ID is transported securely (eg SSL) between the merchant's web site and the customer, for inclusion in the purchase certificate (TC1) and inclusion of the Merchant ID in the secure component of the customer message, allows accurate Merchant ID for payment etc.

4. Customer purchase software confirms debit and requests card reading / swipe. The secure device checks for correct reading of the card.

5. Customer purchase software initiates "GetPIN" to secure device, which encrypts and stores the entered clients PIN.

6. Secure device encrypts PIN and concatenates result with other transaction data. An advanced transaction number is assigned - this may be simply 1, 2, etc, or selected from a more complex predefined set. Concatenated result is cryptographically incorporated into a transaction certificate using a second encryption process. An illustrative transaction certificate is shown in figure 3. This encryption may be, for example, using the public key of an asymmetrical key pair, issued by the device issuer. The secure device is capable of PIN encryption with symmetric double length keys and is capable of encrypting multiple data blocks with a stored protected asymmetric 1024 bit modulus Secure Device Issuer public key half.

Alternatively, the asymmetric public key component may be replaced with a symmetric key derivative of the base key and the random number.

7. Assembled purchase transaction is sent to the merchant, e.g. via email or Internet, see Figure 3 & 4.

8. The transaction may be stored by the merchant for batching into a set of transactions for upload to the acquirer institution. A transaction transfer protocol is designed or exists to satisfy these requirements.

Note: The Merchant may or may not have issued the customer Secure Device reader and / or the customer mag stripe card. In this scenario, it is assumed that the Acquirer has issued neither. Thus, where the Merchant has issued one or both the reader or card, simplification of these steps is possible.

9. The acquirer determines, from for example unencrypted information in the message block, which institution issued the secure device sourcing the transaction. The transaction message provides a Secure Device identifier to be contained within external plain text data, as well as within the certificate.

10. The transaction is forwarded to the secure device issuer, for certificate data recovery, using existing (INTERCHANGE) interbank secure communication systems.

11. The secure device issuer decrypts the certificate data and checks the transaction number against a transaction number database indicating the possible transaction numbers for the device, and which of those transaction numbers have been used. If the transaction number has been used, the device issuer will send a message indicating an error or duplication to the acquiring institution. The entire recovered transaction is now sent to the acquirer, for normal processing and exchange with the issuing institution. The acquirer will then advise the merchant whether funds are cleared or not. The secure device issuer can verify the transaction certificate and check for device transaction duplication (replay) in the transaction number database. The checking application will record the current transaction in the database so it too cannot be duplicated. The transaction will be recovered in an Issuing Institution Security Control Module (card no., $val...etc.).

12. The process proceeds as an existing interchange transaction, via the Acquirer. The secure device issuer can return (interchange) the reconstructed message data to the Acquirer for standard interchange processing.

13. The merchant is informed if the funds are to be forwarded or not. A funds failure mechanism exists to provide the merchant with payment "OK" or "Rejected".

It will be appreciated that many of the elements of the system are already in use, and hence will not be explained further in detail. For example, interbank communications may proceed as normal - the only change is the requirement for involvement by the device issuer. Purchase software is already widely utilised for internet shopping - the only modification required is to ensure adequate security and controls between the software and the secure device. Similarly, the secure device may be merely a simplified version of the card readers currently used for POS transactions.

A key feature of the present invention is that the secure message is assembled by the customer, not the merchant, with a unique identifier for the secure device and for the transaction, as well as the usual PIN inserted by the customer. The probity of intermediaries is not crucial to a secure transaction occurring. The present invention enables the device issuer to identify the source of the message, and verify that replay or duplication of the transaction has not occurred, without any direct communication between the secure device and the issuer. Moreover, no acknowledgment needs to be sent to the issuer's customer, other than a normal statement entry in due course. Even if transactions occur out of order, for example transaction 15 is received by the issuer after transaction 16, the transaction can still proceed and be confirmed as valid - this is not possible with conventional POS systems.

The transaction described above relates to debit transactions - however, it could be applied to credit transactions, or to any other process where it is essential to confirm that the data originated from the correct source, as well as keep the data itself secure, but real time connection is not always possible. Examples include medical and insurance data, confidential reporting and negotiable security instructions.

The present invention fully supports current standards for the interchange of financial institution data, and provides a complete audit trail.

The merchant data is preferably sent to the customer using appropriate encryption established between the merchant and the customer.

There are two relevant forms of encryption. They are Symmetric & Asymmetric respectively.

Symmetric Keys - General

Symmetric encryption uses a common shared key between two parties.

The DES algorithm (Data Encryption Standard - DEA1), has been the accepted means of symmetric encryption, within the Financial Industry.

DES has traditionally used Single Length (8 byte / 64 bit) keys, of which 56 bits are actually used in the encryption process. Because of increases in attacking computer power, single length keys must be extended to double length, using a modified encryption process. The double length key is split into components called Key Left and Key Right.

A double length key is denoted by an asterisk, e.g. *KM1. (This example shows Double length Masterkey number one).

Secure Device Encryption Process

Referring to Figure 2, the top two boxes of this diagram show the device master key. It is a *Master Key. The key is loaded into secure device storage and cannot be recovered or read back outside the device.

PIN Encryption Process for UATEKS

The device *Master Key, (*KM) is loaded by the Secure Device ISSUER, e.g. in this case, the CBA. When required to encrypt an entered PIN, the key is passed through a non linear modification algorithm, seeded by random value (R1).

The resultant derived *Session Key encrypts the PIN:

$C1 = {}^{*}{}_{e}(PIN) = {}_{fn}(R1.{}^{*}KM)$.

The encrypted double length result, C1, together with the random seed, (R1), are stored in the Transaction Certificate generator.

Device Transaction Tracking Process

Each Secure Device will produce a sequentially incremented device transaction number (T1). The device transaction number size will be of sufficient length to allow a reasonable time span of events to be recorded for replay

checking and velocity checking at the host databases. The counter is never reset and only advances in value. At the end of its cycle life, sufficient time will have elapsed for the host database to recognise that roll-over to , for example, 00000000 is a reasonable event span for that particular device.

Each transaction value of (T1) is placed in the Certificate generator.

Magnetic Swipe Track 2 Data

Any transaction will require the user to swipe a card for Track 2 data to be captured. Track 2 data might also be obtained from a smart card file.

Track 2 contains all pertinent data to determine account details. It is protected by placing the entire track 2 data within the Transaction Certificate generator.

Transaction Certificate Generator

Asymmetric Keys

The secure Device will use an asymmetric key half, (PK1), which may be termed the PUBLIC key component.

In reality, this key component need not be public and can be stored, in device secure storage, along with the device master key.

The transaction certificate generator is an asymmetric encryption algorithm within the card reader device. The asymmetric key half (PK1) used to produce the certificate is treated, in the device, as a secure generic key, unique to the Secure Device Issuer.

Note 1: Each Secure Device could have its own unique asymmetric key set. However, this is a waste of resources when the "Public" half of the key can be protected in the same way that the unique device "Master Key is stored. This removes the need for "PK1" certification. Device unique keys would also require additional Issuer host storage space.

Note 2: Alternatively each Secure Device PK1 could be delivered, from the reader device, to an associated terminal PC, together with the assembled content of the generator (Figure 3 illustrates an example TC1 Format). This might permit faster transaction certificate assembly. It would also support a case for a device unique PK1. However, this is not a preferred

method and would greatly reduce the security of the transaction, potentially allowing fund values and Merchant ID etc to be altered.

Note 3: If an asymmetric PK1 is impractical, it is possible to use a symmetric derivative variant of the base key, to produce a signing key in lieu of PK1.

The transaction certificate, TC1, can only be recovered by the Secure Device Issuer. Thus, ALL transactions must come through the device Issuer, before the transaction can be placed into conventional Interchange, for processing.

This would allow selling transactions back to other card issuers, if the Secure Device Issuer were not the Card Issuer as well.

Figure 4 illustrates an example of both a symmetric and asymmetric block message format.

Secure Reader device

The reader device may be purpose built or may be existing technology. The reader can be constructed with a security processor chip capable of operating to industry standards. The encryption processing can be capable of both DES and asymmetric operation. Preferably, the asymmetric key length moduli is 1024 bits. A fixed timing block of output of results may be provided. Device power control might be actuated by e.g. DSR, RTS etc on PC with inbuilt power drop delays etc.

Key Rotation Algorithm

Referring to Figure 5.

Base Key KM: (Reference numeral 1) Consists of a device unique key, 128 bits long. This key is programmed by the Issuer, into each device and also stored in the Issuer OCRF database, protected by a domain master key. (Conventional process). The key is recalled for each PIN decryption process, to derive the session key(s) for the current transaction.

Random Generator R1(L) & R1(R): (Reference numeral 2) The combined random components R1(L) and R1(R) are each a minimum of 64 bits long. the combined 16 byte resultant value is transmitted in the plain text message sent to the Issuer.

Hash Function (#Fn): (Reference numeral 3) Each has function is identical. The 128 bit device key B1 is hashed to 64 bits using the left and right R1 and R2 components respectively. Each 64 bit product is denoted #1L and #2R in Figure 5 schematic. Each 64 bit hash product is then concatenated to produce the final 128 bit session key S1 (reference numeral 4) required by the encrypt function to produce C1 (ΣPIN) in Figure 2.

Hashing Functions are well known to those skilled in the art. The chosen hashing algorithm should be cryptographically robust and may be drawing from, but are not confined to, e.g. SHA or the MD series.

Encryption algorithms are not confined to those described, but should, in any case, be robust and fit for purpose. DES, Triple DES or IDEA are examples applicable to symmetric encryption whereas RSA, LUC or elliptic curve are examples applicable to asymmetric function requirements.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. A system for relatively securely communicating a message from a transmitting means to a receiving means, said transmitting means having a first unique identifier, said message including a second identifier generated by said transmitting means which is unique for each message, wherein said transmitting means encrypts said message, and generates a message block including said encrypted message and said first identifier in unencrypted form, said message block being transmitted, wherein said receiving means is enabled to decrypt the message using the first unique identifier, and includes a list of possible second identifiers for the transmitting means associated with the first identifier, and an indication of whether such second identifiers have been used, so that said message block is recognised as valid only if the second identifier associated with the message block has not previously been used.

2. A system as claimed in claim 1, wherein the encryption is performed using an encryption engine contained within a secure hardware element of the transmitting means.

3. A system as claimed in claim 1 or 2, wherein the encryption engine generates a unique key for each transaction.

4. A system as claimed in claim 3, wherein a second number is transmitted un-encrypted in the message block to the receiving means

5. A system as claimed in claim 4, wherein the receiving means stores decryption information associated with the transmitting means, so that given the first unique identifier and the second number, the message can be decrypted.

6. A system as claimed in claim 4 or 5, wherein the second number associated with each message allows determination as to whether the transaction is legitimate or fraudulent.

7. A method of determining whether a financial transaction is to be approved or rejected in a system of electronic transaction services, the method including the steps of:

checking a transaction number against a transaction number database indicating the possible transaction numbers for a device, the database also indicating which of those transaction numbers have been used, and

if the transaction number has been used, sending a message indicating the transaction is rejected.

8. A method as claimed in claim 7, further including the step of:

determining, from the electronic transaction data which party issued the device sourcing the transaction.

9. A system method or device as herein described.

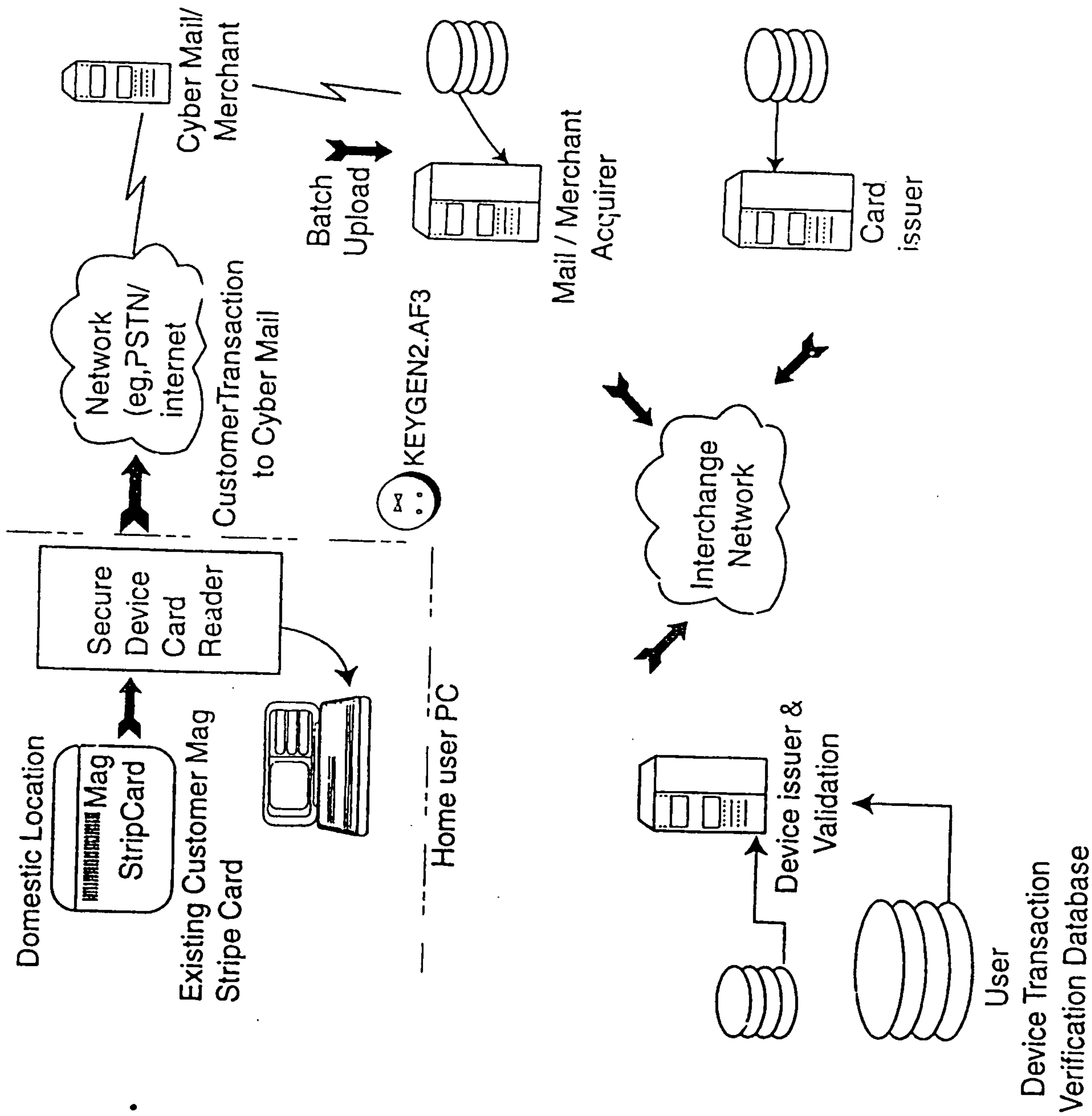

Domestic Location
Mag StripCard
Existing Customer Mag Stripe Card
Secure Device Card Reader
Home user PC
CustomerTransaction to Cyber Mail
Network (eg,PSTN/ internet
KEYGEN2.AF3
Cyber Mail/ Merchant
Batch Upload
Mail / Merchant Acquirer
Card issuer
Interchange Network
Device issuer & Validation
User Device Transaction Verification Database

Fig 1.

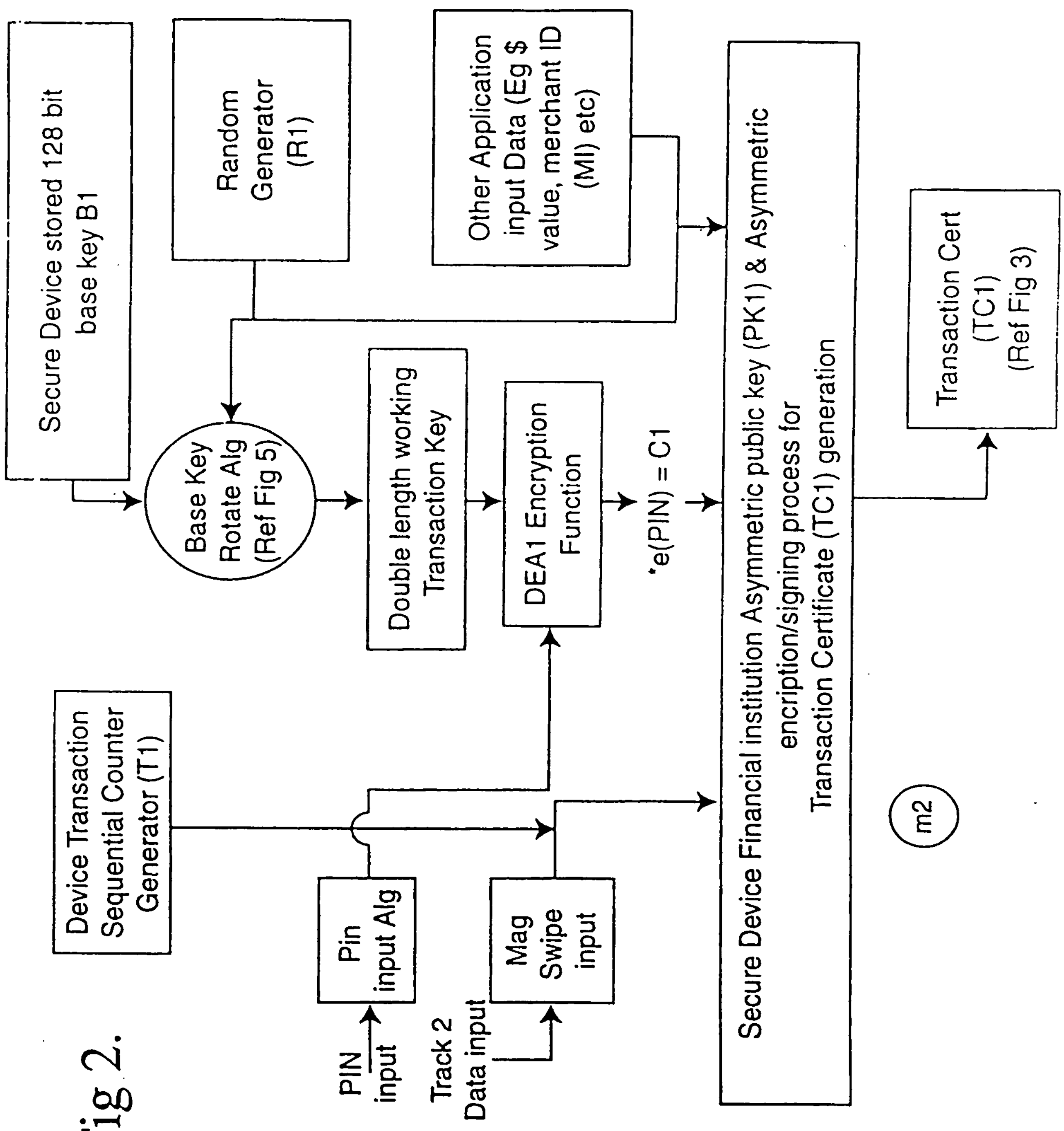

Secure Device stored 128 bit base key B1
Random Generator (R1)
Other Application input Data (Eg $ value, merchant ID (MI) etc)
Base Key Rotate Alg (Ref Fig 5)
Double length working Transaction Key
DEA1 Encryption Function
*e(PIN) = C1
Secure Device Financial institution Asymmetric public key (PK1) & Asymmetric encription/signing process for Transaction Certificate (TC1) generation
Transaction Cert (TC1) (Ref Fig 3)
Device Transaction Sequential Counter Generator (T1)
Pin input Alg
PIN input
Mag Swipe input
Track 2 Data input
m2

Fig 2.

Fig 3.

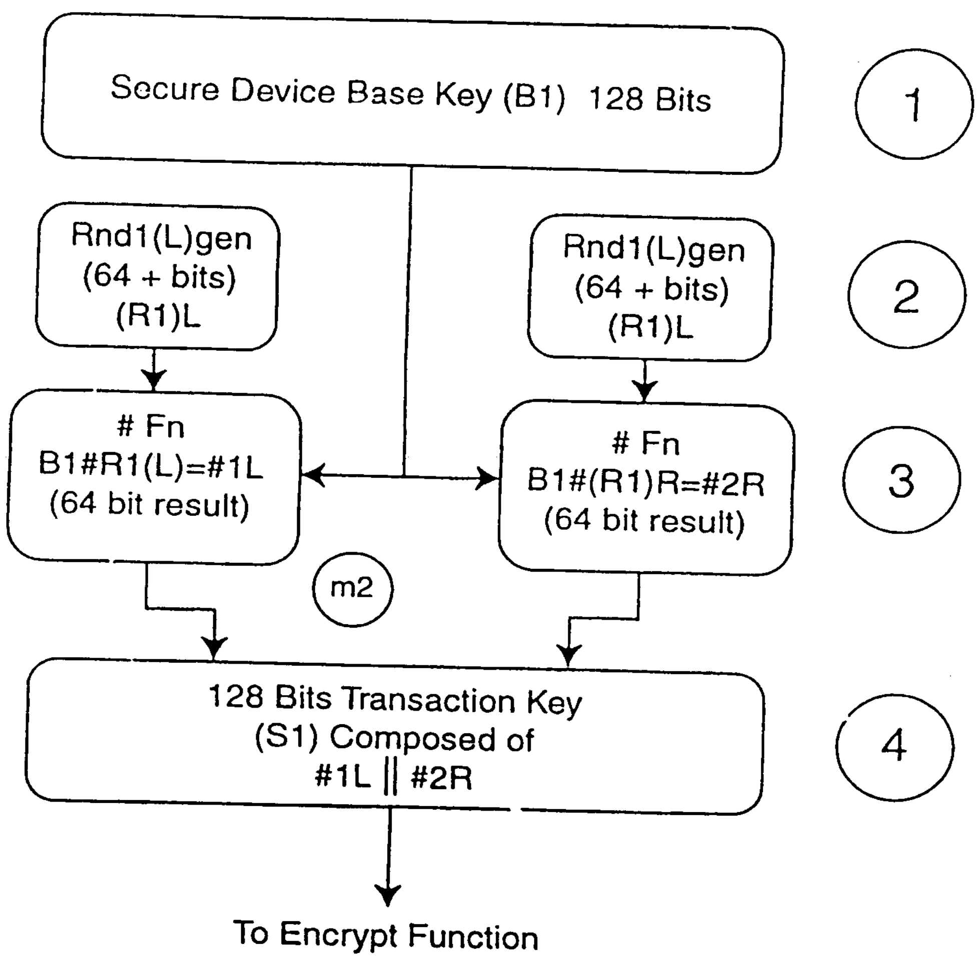
$e_{PK1}[\Sigma PIN \,\|\, \text{Device ID} \,\|\, \text{Track 2} \,\|\, \text{Rnd Gen} \,\|\, \text{Device Tran No} \,\|\, \$ \text{ Value} \,\|\, \text{Merch ID}]$

(C1) (Data) (R1) (T1) (M1)

Fig 4.

TCI Certificate Block || Transactional Plain Text Data Block *(Would requirer Device ID + R1, in plain text, for Symmetric key certificate block version).*

Fig 5.


Secure Device Base Key (B1) 128 Bits
1
Rnd1(L)gen
(64 + bits)
(R1)L
Rnd1(L)gen
(64 + bits)
(R1)L
2
Fn
B1#R1(L)=#1L
(64 bit result)
Fn
B1#(R1)R=#2R
(64 bit result)
3
m2
128 Bits Transaction Key
(S1) Composed of
#1L || #2R
4
To Encrypt Function

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/AU 97/00888

A. CLASSIFICATION OF SUBJECT MATTER

Int Cl[6]: H04L 9/14, 9/20, H04K 1/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC[6]: as above

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
AU IPC: as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPAT (secur:, message:, transact:)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, Y	GB 2309809 (Cer:com Corp.) 6 August 1997 pages 1-6, figure 2	7
Y	US 5 478 994 (Rahman et al) 26 December 1995 Whole document	7

[X] Further documents are listed in the continuation of Box C

[X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 February 1998	17 FEB 1998

Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN INDUSTRIAL PROPERTY ORGANISATION PO BOX 200 WODEN ACT 2606 AUSTRALIA Facsimile No.: (02) 6285 3929	DALE E. SIVER Telephone No.: (02) 6283 2196

C (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, A	WO 97/16902 (Tri-strata) 9 May 1997 Abstract, figures	1, 7
A	WO 95/09500 (Leighton et al) 6 April 1995 Abstract	1, 7
A	EP 197 392 (IBM) 15 October 1986 Columns 1-3	1, 7

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No.
PCT/AU 97/00888

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
GB	2309809	CA	2196356	GB	9601924	GB	9702082
US	5478994	US	5627355				
WO	9716902	AU	23639/97				
WO	9509500	US	5432852				
EP	197392	CA	1249865	DE	3682309	JP	61237546
		US	4649233				

END OF ANNEX